Machine-Learning Based DDOS Attack Classifier in Software Defined Network

Aye Thandar Kyaw
Department of Computer Engineering and Information Technology
Mandalay Technological University
Mandalay, Myanmar
ayethandarkyaw@mtu.edu.mm

May Zin Oo
Department of Computer Engineering and Information Technology
Mandalay Technological University
Mandalay, Myanmar
mayzinoo.dr@gmail.com

Chit Su Khin
Department of Computer Engineering and Information Technology
Mandalay Technological University
Mandalay, Myanmar
chitsukhin922@gmail.com

***Abstract*—Due to centralized control and programmable capability of the SDN architecture, network administrators can easily manage and control the whole network through the centralized controller. According to the SDN architecture, the SDN controller is vulnerable to distributed denial of service (DDOS) attacks. Thus, a failure of SDN controller is a major leak for security concern. The objectives of paper is therefore to detect the DDOS attacks and classify the normal or attack traffic in SDN network using machine learning algorithms. In this proposed system, polynomial SVM is applied to compare to existing linear SVM by using scapy, which is packet generation tool and RYU SDN controller. According to the experimental result, polynomial SVM achieves 3% better accuracy and 34% lower false alarm rate compared to Linear SVM.**

Keywords— DDOS, RYU, SDN, scapy, SVM

I. INTRODUCTION

The new network architecture is Software Defined network (SDN) which is the decoupling of forwarding plane from the control plane. In traditional network architecture, the network devices such as router and switch are managed and controlled by the network administrator according to the devices vendor company. Open Networking Foundation (ONF) [1] develops SDN architecture, where the network administrators perform and manage network service from the centralized SDN controller. Because of the programmability features of SDN, the complex manipulation of network states and the effort of network administrator can be reduced. Then, it makes the user organizations to meet the required function by implementing new Application Programming Interface (API). There are three layers in SDN architecture:

1) Infrastructure layer: This layer is also called a data plane. In this layer, the forwarding devices such as switches and routers can forward and drop incoming packets according to the flow table which is configured by the control plane via southbound interface such as openflow protocol.

2) Control layer: The middle control layer is called control plane. The main function of the control plane is to install the flow rules to the forwarding devices whether the traffic is forwarded or dropped.

3) Application Layer: The upper application layer is also called management plane which gives applications and services over control and infrastructure layer through Representational State Transfer (REST) APIs.

Although SDN has many advantages of centralized and flexible architecture, the separation features of control and data plane make the security challenge for communication organization. The most challenge to SDN architecture is the threat of DDOS attack. The flooding of attack traffic from attackers can overwhelm the forwarding devices and SDN controller tending to the communication system break down.

This paper is composed as follows: Section II discusses the related works associated with many previous researches. Section III explains the effect of the DDOS attack on the SDN network. Section IV expresses the machine learning algorithm used in DDOS attack classifier in SDN network. Section V presents the proposed system framework and implementation. Section VI includes performance evaluation result. Finally, section VII concludes the paper.

II. RELATED WORKS

This section discusses about the DDOS attack detection methods of previous researchers. There are many kinds of DDOS attack detection: entropy-based and machine learning-based method.

A. Entropy-based DDOS Attack Detection

One of the attack detection algorithms in SDN is entropy-based algorithm. The researcher [2] developed the method which not only detects the attacks but also knows the attacking paths and the user could start a mitigation process to provide some degree of protection of the network devices. The proposed method used the entropy variation of destination IP address, flow initiation rate and flow specifications to detect DDOS attack traffic within the short period of time. As soon as attack traffic was generated, the mitigation process was operated to protect the system.

This paper [3] provided a novel stateful SDN approach, StateSec, which used in-switch processing capabilities to detect and mitigate DDOS attacks. This approach monitors packet matching features such as source and destination IP addresses and the source and destination port addresses and then these monitoring features are sent to the entropy-based algorithm to detect and mitigate DDOS attack. The result showed that the detection levels of StateSec was more efficient, very accurate and more precision compared to the sflow.

B. Machine Learning-based DDOS Attack Detection

The researcher [4] used Advanced Support Vector Machine (ASVM) technique to enhance the existing Support Vector

978-1-7281-6486-1/20/$31.00 ©2020 IEEE

Machine (SVM) algorithm. This method proposed the multiclass classification method with three classes for detecting DDOS attack detection. This research was aimed to reduce the training time and testing time by using volumetric and asymmetric features and the dataset was generated by the researcher. According to the experimental result, the detection accuracy of this system was approximately 97%.

Nisharani Meti [5] showed the result by comparing machine learning algorithms: Naïve Bayes, Support Vector Machine (SVM) and Neural Network (NN) classifier to detect the legitimate and illegitimate connection. This paper showed the implementation of the proposed mechanism by using Mininet and Ryu SDN controller on different topologies. According to the experimental result, the author proved that SVM was a better classifier compared to the other two machine learning algorithms.

The researcher [6] designed the SDN framework which consists of traffic collection module, attack identification module and flow table delivery module. The proposed system applied the SVM algorithm for DDOS attack identification and the effectiveness of the result was experimented on the KDD99 dataset. According to the predefined rule, the classification module can identify whether the traffic is attack or normal.

III. DDOS ATTACK ON SDN NETWORK

In SDN network, the controller makes the whole network control decision. The separation framework causes many advantages to the entire network management and improves the network architecture. Because SDN is programmable, flexible, scalable and cost-effective, the business environment using SDN can change their requirements as they like. But, the drawback of SDN centralized architecture is considered as bigger impact than traditional network. So, the most important threat of SDN is DDOS attacks which affect the performance of the entire network and damage the resources of the entire system. The DDOS attack can impact on various places in SDN network. Three main possible places as shown in Fig.1 that can cause DDOS attack are the data plane, the control plane and the secure channel between control and data plane.

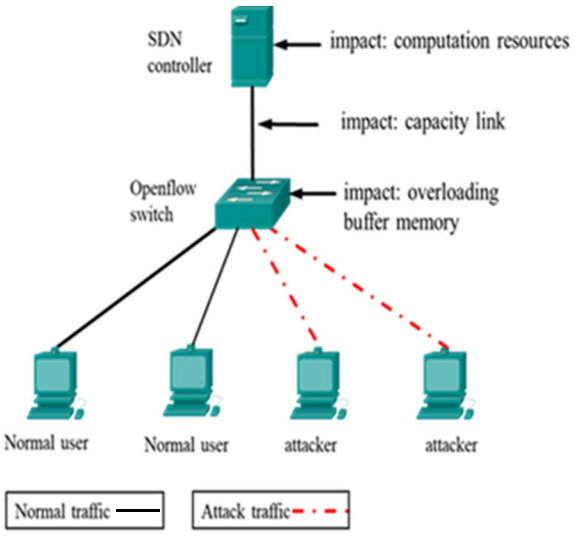

Fig.1. DDOS attack on SDN

IV. DDOS ATTACK DETECTION BASED-ON POLYNOMIAL SUPPORT VECTOR MACHINE (SVM) CLASSIFIER

Support Vector Machine (SVM) is the supervised machine learning model that uses in both classification and regression problems. The SVM [7] is based on the finding the optimal hyperplane separation of labeled instances in a given dataset. The basic idea can be derived by the two-dimensional case of classes.

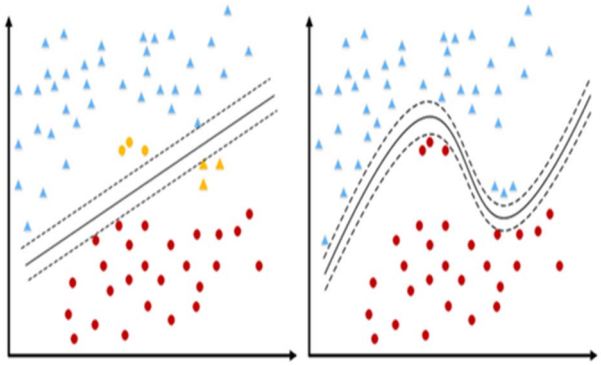

Fig.2. The difference between linear Support Vector Machine and polynomial Support Vector Machine

In the Linear SVM, there is a given dataset D ={(x_1, y_1), (x_2, y2),…… (x_i, y_i)} where x_i is the characteristics vector in a given dataset and y_i is the class lable for the x_i, and y_i indicates two classes +1 (positive class) and -1 (negative class). The set of hyperplanes in SVM can be written as:

$$w.\ x_i + b \geq +1\ ;\ y_i = +1 \quad (1)$$

$$w.\ x_i + b \leq -1;\ y_i = -1 \quad (2)$$

The combination of hyperplanes can be written as the following inequality:

$$y_i\ (w.\ x_i + b) \geq 1;\ 1 \leq i \leq n \quad (3)$$

The optimal problem for the non-separable case can be determined by using slack variables $\xi_i \geq 0$, i =1,…,n which support a hyperplane with minimum errors:

$$\text{minimize: } \frac{1}{2} w^T w + C\sum_{i=1}^{n} \xi i$$

$$\text{subject to } y_i\ (w.\ x_i\ + b) + \xi_i\ \geq 1;\ \xi_i\ \geq 0 \quad (4)$$

where C is regularization parameter which adjusts between the allowed errors in training phase and margin size.

To consider the non-linear case, the kernel function such as polynomial kernel, radial kernel and sigmoid kernel can be used to normalize the feature for the given dataset. Fig.2 shows the difference between linear Support Vector Machine and polynomial Support Vector Machine. In the proposed system, polynomial function is used to compare with existing linear SVM. In the proposed polynomial SVM, the input of the proposed system is flow traffic data and the output result is classified whether the DDOS attack or not. The mathematical expression for the polynomial kernel classifier is given as follow:

$$K\ (x_i, x_j) = (\ x_i\ .\ x_j + 1\ )^d \quad (5)$$

where d is degree of kernel.

V. DDOS ATTACK DETECTION SYSTEM FRAMEWORK

In SDN architecture, the attack can occur at the data plane, control plane and the link between the control and data plane. When the number of incoming new packets from the attacker reaches to the openflow switch, the table-miss event occurs. In this situation, the controller must handle every incoming packet and install new flow rules in switches that consume system resources on the controller and switches. In the proposed system, the DDOS attack classifier is used to handle the attack or normal traffic.

A. Simulation Topology

The network topology is created by using the Miniedit in Mininet Emulator and the proposed system creates tree-type network, which has depth two with nine switches and 64 hosts. The open virtual switch is used for the proposed system. Fig.3 shows the simulation topology of the proposed system. The RYU SDN controller is used and added machine learning algorithm which is accessed for the classification module.

B. Traffic Generation

In the proposed system, the generation of UDP flooding attack traffic and normal traffic are applied to simulate the DDOS attack detection. In the UDP flooding attack, the attack traffic is sent to the victim's host with the random source IP addresses. Scapy is packet generation tool which is written in python programming language. Scapy can handle interactive packet manipulation program and some of the tasks such as forging, tracerouting, scanning, unit test, the network discovery and generating the attack. Scapy is used to generate normal and attack traffic in this proposed system. After the packet is created by using scapy with python, it must be sent to the target destination IP addresses. In this proposed system, packet inter arrival time for UDP attack and normal traffic is assumed as 0.025s and 0.5s respectively**.**

C. Flow Data Collection

For the DDOS attack detection in SDN network, the flow data collection is an important step of the proposed system. The flow status information are stored in the flow table of the openflow switch in SDN network. So, the flow table status information can be collected from the Openflow switch. The flow data can be extracted by sending the flow request command, "sh ovs-ofctl –O openFlow13 dump-flows s1" to the openflow switch. Fig.4. shows the example of the flow status information in a flow table of the openflow switch.

```
mininet> sh ovs-ofctl -O OpenFlow13 dump-flows s1
 OFPST_FLOW reply (OF1.3) (xid=0x2):
cookie=0x0, duration=40.198s, table=0, n_packets=2, n_bytes=196,
priority=1,icmp,nw_src=10.0.0.1,nw_dst=10.0.0.2,actions=output:"s2-
eth2"
 cookie=0x0, duration=40.197s, table=0, n_packets=2, n_bytes=196,
priority=1,icmp,nw_src=10.0.0.2,nw_dst=10.0.0.1,actions=output:"s2-
eth1"
 cookie=0x0, duration=90.026s, table=0, n_packets=27, n_bytes=1926,
priority=0 actions=CONTROLLER:65535
```

Fig.4. Example flow status information of a switch

D. Feature Extraction

After the flow status information is collected, the feature extraction process is performed. The benign and malicious traffic in the SDN network can be collected and analyzed depending on the packet statistic characteristic values from the flow table. According to packet statistic features, whether the attack or not is determined by the proposed system classifier. The extracted features for the proposed system are shown in Table I.

TABLE I. EXTRACTED FEATURES FROM THE FLOW TABLE FOR THE PROPOSED SYSTEM

Features	Description
no_packets	Total packets of the flow
no_bytes	Total bytes of the flow
no_dst	The total number of destination IP address of the flow
duration	The average duration of the flow
Port_no	The total number of used port

E. Implementation of Proposed System

In this proposed system, two machine learning algorithms are used as a comparative experiment for DDOS attack detection. Firstly, one RYU SDN controller is implemented by using the python program in linux environment. Nine openflow virtual switches and 64 hosts are created in Mininet GUI. In the proposed system, the normal and attack traffic are simultaneously generated to the hosts. Normal traffic is generated from one of the hosts to all with random source IP addresses. Similarly, attack traffic is run from one of the hosts with the single victim IP address or multi-victims IP addresses while other hosts are running in normal traffic. In the experimental environment, when the attack traffic from one host reaches to the openflow switch, the switch sends packet-in message to the controller for requesting for the new flow rule. Once the controller receives higher number of packet-in messages, the machine learning algorithm with the RYU SDN controller classifies whether the incoming traffic is attack or normal depending on the traffic features.

VI. PERFORMANCE EVALUATION RESULT

The proposed system is tested by using two machine learning algorithms which are existing linear SVM and polynomial SVM algorithm. The dataset for the proposed system is collected by generating volume-based DDOS attack traffic and normal traffic. The user-simulated dataset with the total of 650 instances of benign traffic and malicious traffic are created by using scapy packet generation tool. In this proposed system, experimental result can be measured by the accuracy, false alarm rate, detection rate and precision. So, performance evaluation metrics are shown in the following equations:

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (6)$$

$$\text{False Alarm Rate} = \frac{FP}{FP+TN} \times 100 \quad (7)$$

$$\text{Detection Rate} = \frac{TP}{TP+FN} \times 100 \quad (8)$$

$$\text{Precision} = \frac{TP}{TP+FP} \times 100 \quad (9)$$

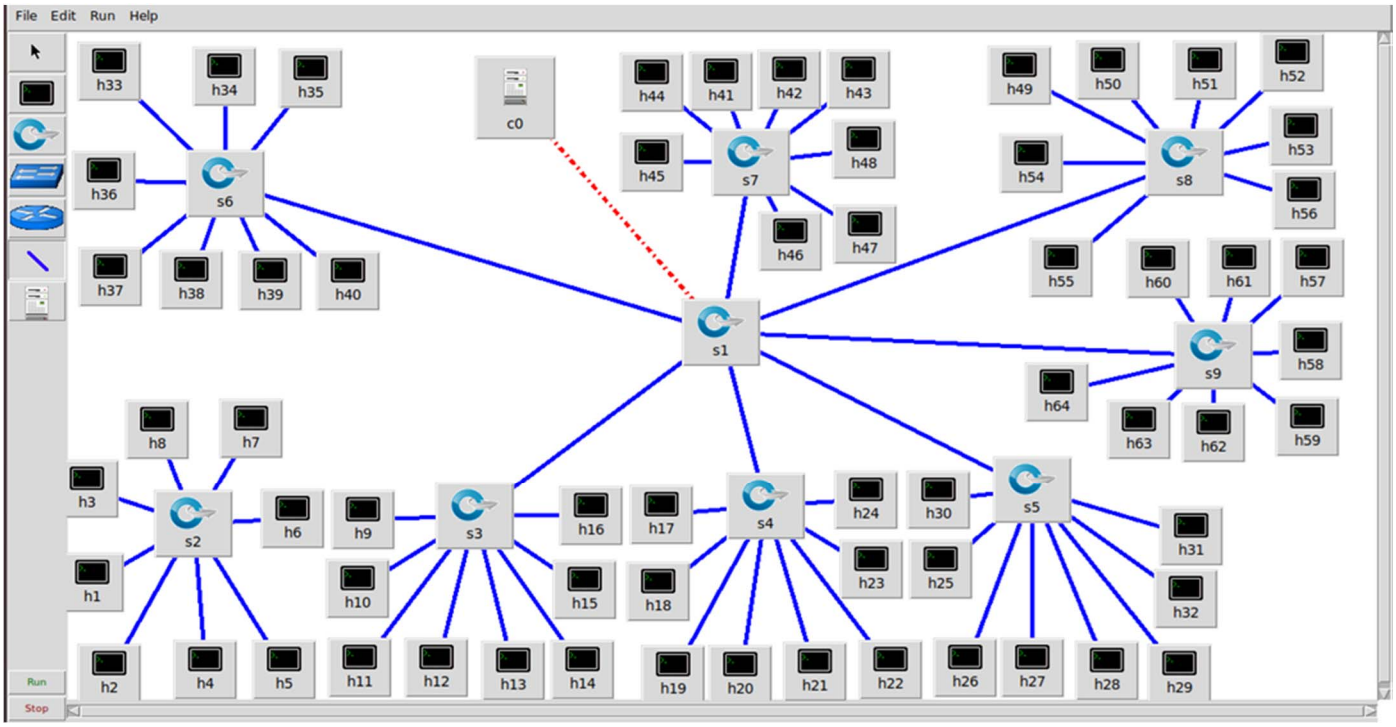

Fig.3. Simulation topology in Miniedit GUI

where TP means the total number of malicious traffic that are correctly classified as malicious traffic and FN means the total number of malicious traffic that are incorrectly classified as normal traffic. FP means the total number of normal traffic that are incorrectly classified as malicious traffic and TN means the total number of normal traffic that are correctly classified as normal.

Table II shows performance evaluation comparison for linear SVM and polynomial SVM classifier. When calculating the percentage difference of evaluation results, the polynomial SVM classifier can outperform than linear SVM in all performance measures within the range of 3% minimum and 34% maximum. Also, the precision rate of polynomial SVM is more precise than linear SVM.

TABLE II. PERFORMANCE EVALUATION COMPARISON

Classifier	Accuracy	Average detection rate	Average false alarm rate	Precision
Polynomial SVM	95.38%	96.03%	5.05%	95.05 %
Linear SVM	92.85%	92.85%	7.15%	91.15 %

VII. CONCLUSIONS

Software Defined Networking is based on the programmable, centralized controller which supports the adaptable nature of network functions. According to the architecture, the important threat of the SDN network is security issue. So, this paper is designed and implemented DDOS attack detection method in SDN network. The proposed system consists of traffic data collection, feature extraction and attack classification and applies the polynomial SVM algorithm. According to the evaluation result, the proposed system is able to classify DDOS flooding attack with about 95% average accuracy and 5% false alarm rate using polynomial SVM classifier. By comparing with the linear SVM classifier, the proposed classifier is more accurate and lower false alarm rate.

REFERENCES

[1] Open networking foundation. [Online]. Available: https://www.opennetworking.org.

[2] M.Kia, “Early detection and mitigation of DDoS attacks in software defined networks”, M.Sc. Thesis. Ryerson University, Toronto, Ontario, Canada, 2015.

[3] J.Boite, P.A.Nardin, F.Rebecchi, M.Bouet, V.Conan, “StateSec: Stateful monitoring for DDoS protection in software defined networks”,IEEE Conference on Network Softwarization, Bologna,Italy, 2017

[4] M. Myint Oo, K. Sinchai, and K. ossaporn, “ Advanced support vector machine based detection for distributed denial of service attack on software defined network,” Journal of Computer Networks and Communications, Volume 2019. https://doi.org/10.1155/2019/8012568

[5] N. Meti, D.G Narayan,V.P Baligar,"Detection of distributed denial of service attacks using machine learning algorithms in SDN",IEEE 2017.

[6] Y. Lingfeng, Z. Hui, “DDoS attack identification and defense using SDN based on machine learning method”, DOI 10.1109/I-SPAN.2018, IEEE.

[7] M. Latah , L. Toker ,"A novel intelligent approach for detecting DoS flooding attacks in software-defined networks", IJAIN, volume 4, march 2018,pp11-20.

[8] Mininet home page[online]. Available:http://mininet.org

[9] RYU controller [online]. Avaialble:https://osrg.github.io/ryu